# Quantum Enabled Security (QES) for Optical Communications

July 10, 2013

## Quantum Enabled Security (QES) for Optical Communications

Applications:

- Secure communication over optical or free space networks
- Financial networks
- Transparent access networks: fiber to the home (FTTH); fiber to the premises (FTTP); passive optical networks (PONs)
- Multi-party quantum communications
- Avionics
- Constrained environments such as: government agencies; the U.S. Embassy; and military aircraft

Benefits:

- Future-proof security into the future, guaranteed by the laws of nature
- Dedicated fiber optics or designated channel not required
- Existing infrastructure used
- Protection against tapping, jamming, or denial-of-service (DoS) attacks
- Multi-level security, access control, authentication, anonymous routing, and privacy protection
- Invulnerable to both conventional and quantum computer attacks
- Quantum enabled security applied at the photonic layer

Summary:

In today's technological world, the information passed through optical fiber networks every second is as valuable as currency. But often security isn't adequate for the growing network capabilities and the threats against them. Optical fiber networks can be "tapped" with commercially available equipment. Networks can be disrupted with methods as simple as introducing noise to tie up resources, increasing eavesdropping opportunities. Passwords and security tokens used for authentication and access control are continually proven to be inadequate against both external and internal threats.

In response to ever-increasing cybersecurity threats, Los Alamos National Laboratory has developed Quantum Enabled Security (QES), a revolutionary new cybersecurity capability using quantum (single-photon) communications integrated with optical communications to

provide a strong, innate, security foundation at the photonic layer for optical fiber networks. In QES, quantum communications are established using secret random numbers shared between authorized users. These numbers are used to generate constantly changing secret codes to spread conventional communications in time and/or frequency. Without knowledge of the spreading codes, adversaries cannot determine where the QES communications are located in time or frequency and are unable to discern or tap these communications. In contrast, the intended recipients share the secret spreading codes with the sender, who can "de-spread" the signals and recover the data faithfully. True random numbers produced by quantum communication are essential to prevent adversaries from determining spreading codes by long-term monitoring.

QES multi-party quantum communications protocols also allow the formation of ad hoc coalitions of users, with the communications of different groups separated and protected through the use of orthogonal, secret spreading codes. These protocols leverage the network to deliver quantum-enabled security between users who may not have direct quantum communications.

Because only users aware of the spreading codes can communicate, the QES methodology provides other desirable network security services in addition to privacy, including authentication, anonymous routing, access control, and protection against denial-ofservice attacks. While revolutionary in conception, the QES methodology can be implemented as an overlay on existing campus, enterprise, or metro-area transparent networks, with node-to-node path lengths as large as 60 kilometers using current technology. By extending security services to the photonic foundation of network communications, the QES enables a more robust, assured cybersecurity in optical fiber networks and makes many new security paradigms possible.

Development Stage:

Technology Readiness Level: 4 - Component prototypes tested in a controlled environment

Patent Status:

Quantum Enabled Security for Optical Communication, U.S. Patent Application No. 12/638,730 (DOE S-116,328), Patent Application Filing Date: December 15, 2009

Licensing Status:

Available for exclusive or non-exclusive licensing and collaborative agreements.

For more information, contact Licensing@lanl.gov.

---

**RICHARD P. FEYNMAN CENTER FOR INNOVATION**

www.lanl.gov/feynmancenter | (505) 667-9090 | feynmancenter@lanl.gov